Gestionar grupos y usuarios

StorageGRID 11.8

NetApp
March 19, 2024

Tabla de contenidos

Gestionar grupos y usuarios

Usar la federación de identidades

El uso de la federación de identidades agiliza la configuración de usuarios y grupos de inquilinos, y permite a los usuarios de inquilinos iniciar sesión en la cuenta de inquilinos utilizando credenciales conocidas.

Configurar la federación de identidades para el Administrador de inquilinos

Puede configurar la federación de identidades para el administrador de inquilinos si desea que los grupos de inquilinos y los usuarios se gestionen en otro sistema como Active Directory, Azure Active Directory (Azure AD), OpenLDAP u Oracle Directory Server.

Antes de empezar

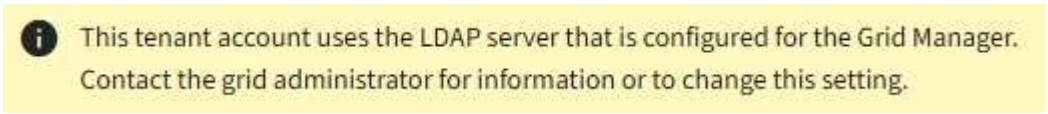
- Ha iniciado sesión en el administrador de inquilinos mediante un "navegador web compatible".
- Pertenece a un grupo de usuarios que tiene el "Permiso de acceso raíz".
- Se utiliza Active Directory, Azure AD, OpenLDAP u Oracle Directory Server como proveedor de identidades.

  Si desea utilizar un servicio LDAP v3 que no esté en la lista, póngase en contacto con el soporte técnico.

- Si planea utilizar OpenLDAP, debe configurar el servidor OpenLDAP. Consulte Instrucciones para configurar el servidor OpenLDAP.
- Si planea utilizar la seguridad de la capa de transporte (TLS) para las comunicaciones con el servidor LDAP, el proveedor de identidades debe usar TLS 1.2 o 1.3. Consulte "Cifrados compatibles para conexiones TLS salientes".

Acerca de esta tarea

Si puede configurar un servicio de federación de identidades para su inquilino depende de cómo se haya configurado su cuenta de inquilino. Es posible que el inquilino comparta el servicio de federación de identidades configurado para Grid Manager. Si ve este mensaje cuando accede a la página Identity Federation, no puede configurar un origen de identidad federado independiente para este arrendatario.

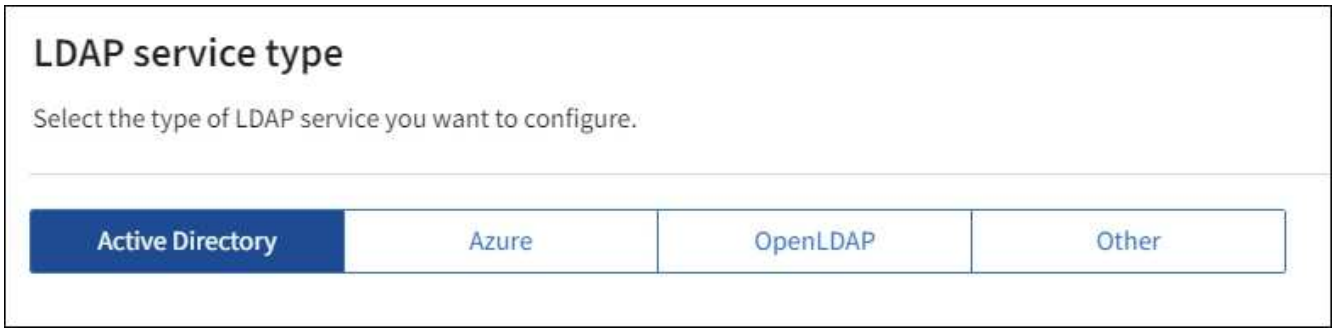


Introducir configuración

Al configurar Identify federation, proporciona los valores que StorageGRID necesita para conectarse a un servicio LDAP.

Pasos

1. Seleccione **ADMINISTRACIÓN de ACCESO** > **federación de identidades**.
2. Seleccione **Activar federación de identidades**.
3. En la sección Tipo de servicio LDAP, seleccione el tipo de servicio LDAP que desea configurar.



Seleccione **otros** para configurar valores para un servidor LDAP que utilice Oracle Directory Server.

4. Si ha seleccionado **otros**, complete los campos de la sección atributos LDAP . De lo contrario, vaya al paso siguiente.
   - **Nombre único de usuario**: Nombre del atributo que contiene el identificador único de un usuario LDAP. Este atributo es equivalente a. `sAMAccountName` Para Active Directory y. `uid` Para OpenLDAP. Si va a configurar Oracle Directory Server, introduzca `uid`.
   - **UUID de usuario**: Nombre del atributo que contiene el identificador único permanente de un usuario LDAP. Este atributo es equivalente a. `objectGUID` Para Active Directory y. `entryUUID` Para OpenLDAP. Si va a configurar Oracle Directory Server, introduzca `nsuniqueid`. El valor de cada usuario para el atributo especificado debe ser un número hexadecimal de 32 dígitos en formato de 16 bytes o de cadena, donde se ignoran los guiones.
   - **Nombre único del grupo**: Nombre del atributo que contiene el identificador único de un grupo LDAP. Este atributo es equivalente a. `sAMAccountName` Para Active Directory y. `cn` Para OpenLDAP. Si va a configurar Oracle Directory Server, introduzca `cn`.
   - **UUID de grupo**: Nombre del atributo que contiene el identificador único permanente de un grupo LDAP. Este atributo es equivalente a. `objectGUID` Para Active Directory y. `entryUUID` Para OpenLDAP. Si va a configurar Oracle Directory Server, introduzca `nsuniqueid`. El valor de cada grupo para el atributo especificado debe ser un número hexadecimal de 32 dígitos en formato de 16 bytes o de cadena, donde se ignoran los guiones.
5. Para todos los tipos de servicio LDAP, introduzca la información de servidor LDAP y conexión de red necesaria en la sección Configure LDAP Server.
   - **Hostname**: El nombre de dominio completo (FQDN) o la dirección IP del servidor LDAP.
   - **Puerto**: El puerto utilizado para conectarse al servidor LDAP.

     El puerto predeterminado para STARTTLS es 389 y el puerto predeterminado para LDAPS es 636. Sin embargo, puede utilizar cualquier puerto siempre que su firewall esté configurado correctamente.

   - **Nombre de usuario**: La ruta completa del nombre completo (DN) para el usuario que se conectará al servidor LDAP.

     Para Active Directory, también puede especificar el nombre de inicio de sesión de nivel inferior o el nombre principal del usuario.

     El usuario especificado debe tener permiso para enumerar grupos y usuarios y para tener acceso a los siguientes atributos:

     - `sAMAccountName` o. `uid`

- `objectGUID`, `entryUUID`, o. `nsuniqueid`
- `cn`
- `memberOf` o. `isMemberOf`
- **Active Directory**: `objectSid`, `primaryGroupID`, `userAccountControl`, y. `userPrincipalName`
- **Azure**: `accountEnabled` y.. `userPrincipalName`

◦ **Contraseña**: La contraseña asociada al nombre de usuario.

> Si cambia la contraseña en el futuro, debe actualizarla en esta página.

◦ **DN base de grupo**: La ruta completa del nombre distinguido (DN) para un subárbol LDAP que desea buscar grupos. En el ejemplo de Active Directory (a continuación), se pueden usar como grupos federados todos los grupos cuyo nombre distintivo sea relativo al DN base (DC=storagegrid,DC=example,DC=com).

> Los valores de **Nombre único de grupo** deben ser únicos dentro del **DN base de grupo** al que pertenecen.

◦ **DN base de usuario**: La ruta completa del nombre completo (DN) de un subárbol LDAP que desea buscar usuarios.

> Los valores de **Nombre único de usuario** deben ser únicos dentro del **DN base de usuario** al que pertenecen.

◦ **Formato de nombre de usuario de enlace** (opcional): El patrón de nombre de usuario predeterminado StorageGRID debe usarse si el patrón no se puede determinar automáticamente.

Se recomienda proporcionar **Formato de nombre de usuario Bind** porque puede permitir que los usuarios inicien sesión si StorageGRID no puede enlazar con la cuenta de servicio.

Introduzca uno de estos patrones:

- **Patrón UserPrincipalName (Active Directory y Azure)**: `[USERNAME]@*example*.com`
- **Patrón de nombre de inicio de sesión de nivel inferior (Active Directory y Azure)**: `*example*\[USERNAME]`
- **Patrón de nombre completo**: `CN=[USERNAME],CN=Users,DC=*example*,DC=com`

  Incluya **[USERNAME]** exactamente como está escrito.

6. En la sección Seguridad de la capa de transporte (TLS), seleccione una configuración de seguridad.
   ◦ **Use STARTTLS**: Utilice STARTTLS para asegurar las comunicaciones con el servidor LDAP. Esta es la opción recomendada para Active Directory, OpenLDAP u otros, pero esta opción no es compatible con Azure.
   ◦ **Use LDAPS**: La opción LDAPS (LDAP sobre SSL) utiliza TLS para establecer una conexión con el servidor LDAP. Debe seleccionar esta opción para Azure.
   ◦ **No utilice TLS**: El tráfico de red entre el sistema StorageGRID y el servidor LDAP no estará protegido. Esta opción no es compatible con Azure.

El uso de la opción **no usar TLS** no es compatible si el servidor de Active Directory aplica la firma LDAP. Debe usar STARTTLS o LDAPS.

7. Si seleccionó STARTTLS o LDAPS, elija el certificado utilizado para proteger la conexión.
   - **Utilizar certificado CA del sistema operativo**: Utilice el certificado predeterminado de CA de red instalado en el sistema operativo para asegurar las conexiones.
   - **Utilizar certificado de CA personalizado**: Utilice un certificado de seguridad personalizado.

     Si selecciona esta opción, copie y pegue el certificado de seguridad personalizado en el cuadro de texto del certificado de CA.

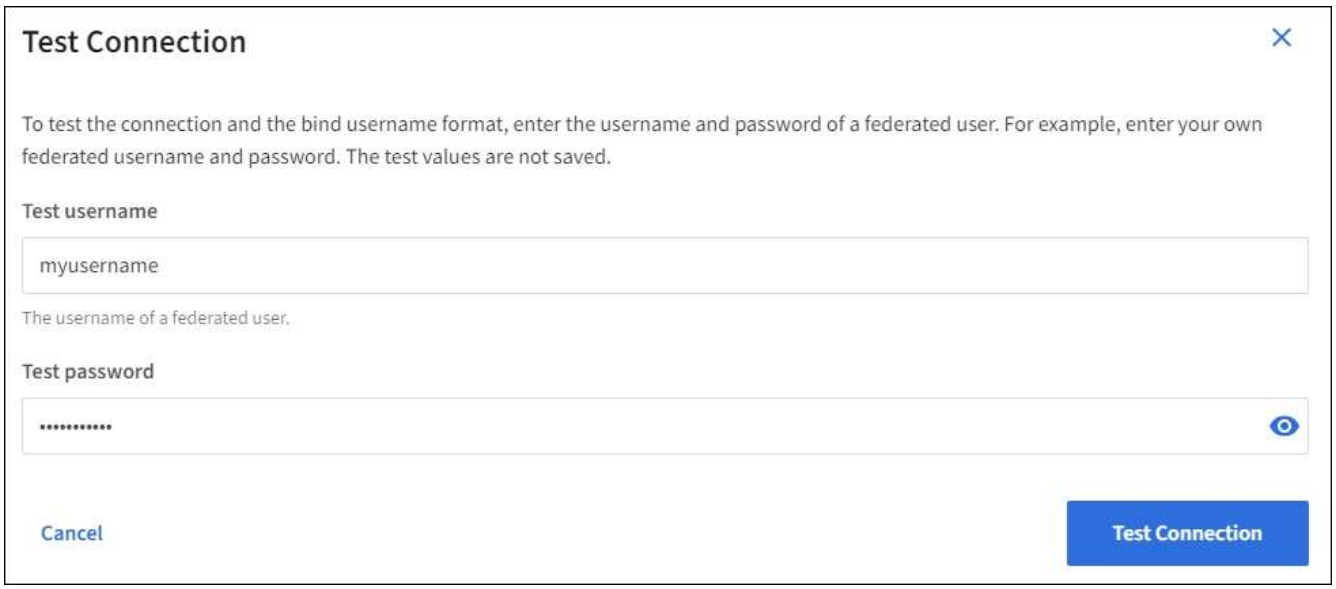
Pruebe la conexión y guarde la configuración

Después de introducir todos los valores, es necesario probar la conexión para poder guardar la configuración. StorageGRID verifica la configuración de conexión del servidor LDAP y el formato de nombre de usuario de enlace, si proporcionó uno.

Pasos

1. Seleccione **probar conexión**.
2. Si no se proporciona un formato de nombre de usuario de enlace:
   - Si la configuración de conexión es válida, aparecerá un mensaje que indica que la conexión se ha realizado correctamente. Seleccione **Guardar** para guardar la configuración.
   - Si la configuración de conexión no es válida, aparecerá un mensaje que indica que no se ha podido establecer la conexión de prueba. Seleccione **Cerrar**. Luego, resuelva cualquier problema y vuelva a probar la conexión.
3. Si proporcionó un formato de nombre de usuario de enlace, introduzca el nombre de usuario y la contraseña de un usuario federado válido.

   Por ejemplo, introduzca su propio nombre de usuario y contraseña. No incluya ningún carácter especial en el nombre de usuario, como @ o /.



   - Si la configuración de conexión es válida, aparecerá un mensaje que indica que la conexión se ha realizado correctamente. Seleccione **Guardar** para guardar la configuración.

- Aparecerá un mensaje de error si las opciones de conexión, el formato de nombre de usuario de enlace o el nombre de usuario y la contraseña de prueba no son válidos. Resuelva los problemas y vuelva a probar la conexión.

Forzar la sincronización con el origen de identidades

El sistema StorageGRID sincroniza periódicamente grupos federados y usuarios del origen de identidades. Puede forzar el inicio de la sincronización si desea habilitar o restringir los permisos de usuario lo antes posible.

Pasos

1. Vaya a la página federación de identidades.
2. Seleccione **servidor de sincronización** en la parte superior de la página.

   El proceso de sincronización puede tardar bastante tiempo en función del entorno.

   La alerta **fallo de sincronización de la federación de identidades** se activa si hay un problema al sincronizar grupos federados y usuarios del origen de identidades.

Deshabilitar la federación de identidades

Puede deshabilitar temporalmente o de forma permanente la federación de identidades para grupos y usuarios. Cuando la federación de identidades está deshabilitada, no existe comunicación entre StorageGRID y el origen de identidades. Sin embargo, cualquier configuración que haya configurado se conservará, lo que le permitirá volver a habilitar fácilmente la federación de identidades en el futuro.

Acerca de esta tarea

Antes de deshabilitar la federación de identidades, debe tener en cuenta lo siguiente:

- Los usuarios federados no podrán iniciar sesión.
- Los usuarios federados que hayan iniciado sesión en ese momento, retendrán el acceso al sistema StorageGRID hasta que caduque la sesión, pero no podrán iniciar sesión después de que caduque la sesión.
- No se realizará la sincronización entre el sistema StorageGRID y el origen de identidad, y no se realizarán alertas ni alarmas para las cuentas que no se hayan sincronizado.
- La casilla de verificación **Habilitar federación de identidad** está desactivada si el inicio de sesión único (SSO) está configurado en **enabled** o **Sandbox Mode**. El estado de SSO de la página Single Sign-On debe ser **Desactivado** antes de poder deshabilitar la federación de identidades. Consulte "Desactive el inicio de sesión único".

Pasos

1. Vaya a la página federación de identidades.
2. Desmarque la casilla de verificación **Habilitar federación de identidad**.

Instrucciones para configurar el servidor OpenLDAP

Si desea utilizar un servidor OpenLDAP para la federación de identidades, debe configurar ajustes específicos en el servidor OpenLDAP.

En el caso de fuentes de identidad que no sean ActiveDirectory ni Azure, StorageGRID no bloqueará automáticamente el acceso S3 a los usuarios que estén deshabilitados externamente. Para bloquear el acceso a S3, elimine cualquier clave S3 para el usuario o elimine al usuario de todos los grupos.

Revestimientos memberOf y reft

Se deben habilitar las superposiciones memberof y reft. Para obtener más información, consulte las instrucciones para el mantenimiento de miembros del grupo inverso en "Documentación de OpenLDAP: Guía del administrador de la versión 2.4".

Indización

Debe configurar los siguientes atributos OpenLDAP con las palabras clave de índice especificadas:

- `olcDbIndex: objectClass eq`
- `olcDbIndex: uid eq,pres,sub`
- `olcDbIndex: cn eq,pres,sub`
- `olcDbIndex: entryUUID eq`

Además, asegúrese de que los campos mencionados en la ayuda para Nombre de usuario estén indexados para un rendimiento óptimo.

Consulte la información sobre el mantenimiento de pertenencia a grupos inversa en la "Documentación de OpenLDAP: Guía del administrador de la versión 2.4".

Gestionar grupos de inquilinos

Cree grupos para un inquilino de S3

Es posible gestionar permisos para grupos de usuarios S3 importando grupos federados o creando grupos locales.

Antes de empezar

- Ha iniciado sesión en el administrador de inquilinos mediante un "navegador web compatible".
- Pertenece a un grupo de usuarios que tiene el "Permiso de acceso raíz".
- Si planea importar un grupo federado, tiene "federación de identidades configurada", y el grupo federado ya existe en el origen de identidad configurado.
- Si su cuenta de inquilino tiene el permiso **Use grid federation connection**, ha revisado el flujo de trabajo y las consideraciones para "clonación de usuarios y grupos de inquilinos", y ha iniciado sesión en la cuadrícula de origen del inquilino.

Acceda al asistente Crear grupo

Como primer paso, acceda al asistente de creación de grupos.

Pasos

1. Seleccione **ADMINISTRACIÓN de ACCESO** > **grupos**.

2. Si su cuenta de inquilino tiene el permiso **Usar conexión de federación de grid**, confirme que aparece un banner azul, indicando que los nuevos grupos creados en esta cuadrícula se clonarán en el mismo inquilino en la otra cuadrícula de la conexión. Si este banner no aparece, puede que haya iniciado sesión en la cuadrícula de destino del inquilino.

3. Seleccione **Crear grupo**.

Elija un tipo de grupo

Puede crear un grupo local o importar un grupo federado.

Pasos

1. Seleccione la ficha **Grupo local** para crear un grupo local o seleccione la ficha **Grupo federado** para importar un grupo desde el origen de identidad configurado previamente.

   Si se ha habilitado el inicio de sesión único (SSO) para el sistema StorageGRID, los usuarios que pertenecen a grupos locales no podrán iniciar sesión en el Gestor de inquilinos, aunque puedan utilizar las aplicaciones cliente para gestionar los recursos del inquilino, en función de los permisos de grupo.

2. Introduzca el nombre del grupo.
   - **Grupo local**: Introduzca tanto un nombre para mostrar como un nombre exclusivo. Puede editar el nombre para mostrar más adelante.

     > Si su cuenta de inquilino tiene el permiso **Usar conexión de federación de grid**, se producirá un error de clonación si el mismo **nombre único** ya existe para el inquilino en la cuadrícula de destino.

   - **Grupo federado**: Introduzca el nombre único. Para Active Directory, el nombre único es el nombre asociado con `sAMAccountName` atributo. Para OpenLDAP, el nombre único es el nombre asociado con `uid` atributo.
3. Seleccione **continuar**.

Administrar permisos de grupo

Los permisos de grupo controlan las tareas que los usuarios pueden realizar en el gestor de inquilinos y en la API de gestión de inquilinos.

Pasos

1. Para **Modo de acceso**, seleccione una de las siguientes opciones:
   - **Read-write** (por defecto): Los usuarios pueden iniciar sesión en Tenant Manager y administrar la configuración del inquilino.
   - **Sólo lectura**: Los usuarios sólo pueden ver los ajustes y las funciones. No pueden hacer ningún cambio ni realizar ninguna operación en el administrador de inquilinos o la API de gestión de inquilinos. Los usuarios locales de solo lectura pueden cambiar sus propias contraseñas.

   > Si un usuario pertenece a varios grupos y cualquier grupo está establecido en sólo lectura, el usuario tendrá acceso de sólo lectura a todos los ajustes y características seleccionados.

2. Seleccione uno o más permisos para este grupo.

   Consulte "Permisos de gestión de inquilinos".

3. Seleccione **continuar**.

Establezca la política de grupo S3

La política de grupo determina qué permisos de acceso S3 tendrán los usuarios.

Pasos

1. Seleccione la política que desea usar para este grupo.

Política de grupo	Descripción
Sin acceso S3	Predeterminado. Los usuarios de este grupo no tienen acceso a los recursos de S3, a menos que el acceso se conceda con una política de bloque. Si selecciona esta opción, de forma predeterminada, solo el usuario raíz tendrá acceso a recursos de S3.
Acceso de sólo lectura	Los usuarios de este grupo tienen acceso de solo lectura a los recursos de S3. Por ejemplo, los usuarios de este grupo pueden enumerar objetos y leer datos de objetos, metadatos y etiquetas. Cuando selecciona esta opción, la cadena JSON para una política de grupo de solo lectura aparece en el cuadro de texto. No puede editar esta cadena.
Acceso total	Los usuarios de este grupo tienen acceso completo a recursos de S3, incluidos los bloques. Cuando selecciona esta opción, la cadena JSON para una política de grupo de acceso completo aparece en el cuadro de texto. No puede editar esta cadena.

Política de grupo	Descripción
Mitigación del ransomware	Esta política de ejemplo se aplica a todos los depósitos de este inquilino. Los usuarios de este grupo pueden realizar acciones comunes, pero no pueden suprimir de forma permanente objetos de los bloques que tienen activado el control de versiones de objetos. Los usuarios del administrador de inquilinos que tienen el permiso **Administrar todos los cubos** pueden anular esta política de grupo. Limite el permiso Gestionar todos los buckets a usuarios de confianza y use la autenticación multifactor (MFA) cuando esté disponible.
Personalizado	A los usuarios del grupo se les conceden los permisos que especifique en el cuadro de texto.

2. Si ha seleccionado **personalizado**, introduzca la directiva de grupo. Cada política de grupo tiene un límite de tamaño de 5,120 bytes. Debe introducir una cadena con formato JSON válida.

   Para obtener información detallada sobre las políticas de grupo, incluida la sintaxis del idioma y los ejemplos, consulte "Ejemplo de políticas de grupo".

3. Si está creando un grupo local, seleccione **continuar**. Si está creando un grupo federado, seleccione **Crear grupo** y **Finalizar**.

Añadir usuarios (sólo grupos locales)

Puede guardar el grupo sin agregar usuarios o, opcionalmente, puede agregar cualquier usuario local que ya exista.

> Si su cuenta de inquilino tiene el permiso **Usar conexión de federación de grid**, los usuarios que seleccione al crear un grupo local en la cuadrícula de origen no se incluyen cuando el grupo se clona en la cuadrícula de destino. Por este motivo, no seleccione usuarios al crear el grupo. En su lugar, seleccione el grupo cuando cree los usuarios.

Pasos

1. Opcionalmente, seleccione uno o varios usuarios locales para este grupo.
2. Seleccione **Crear grupo** y **Finalizar**.

   El grupo creado aparece en la lista de grupos.

   Si su cuenta de inquilino tiene el permiso **Use grid federation connection** y usted está en la cuadrícula de origen del inquilino, el nuevo grupo se clona en la cuadrícula de destino del inquilino. **Success** aparece como **Cloning status** en la sección Overview de la página de detalles del grupo.

Cree grupos para un inquilino de Swift

Es posible gestionar los permisos de acceso para una cuenta de inquilino de Swift mediante la importación de grupos federados o la creación de grupos locales. Al menos un grupo debe tener el permiso de administrador de Swift, que se requiere para gestionar los contenedores y los objetos de una cuenta de inquilino de Swift.

Se eliminó la compatibilidad con aplicaciones cliente de Swift y se quitará en unas versiones futuras.

Antes de empezar

- Ha iniciado sesión en el administrador de inquilinos mediante un "navegador web compatible".
- Pertenece a un grupo de usuarios que tiene el "Permiso de acceso raíz".
- Si planea importar un grupo federado, tiene "federación de identidades configurada", y el grupo federado ya existe en el origen de identidad configurado.

Acceda al asistente Crear grupo

Pasos

Como primer paso, acceda al asistente de creación de grupos.

1. Seleccione **ADMINISTRACIÓN de ACCESO** > **grupos**.
2. Seleccione **Crear grupo**.

Elija un tipo de grupo

Puede crear un grupo local o importar un grupo federado.

Pasos

1. Seleccione la ficha **Grupo local** para crear un grupo local o seleccione la ficha **Grupo federado** para importar un grupo desde el origen de identidad configurado previamente.

   Si se ha habilitado el inicio de sesión único (SSO) para el sistema StorageGRID, los usuarios que pertenecen a grupos locales no podrán iniciar sesión en el Gestor de inquilinos, aunque puedan utilizar las aplicaciones cliente para gestionar los recursos del inquilino, en función de los permisos de grupo.

2. Introduzca el nombre del grupo.
   - **Grupo local**: Introduzca tanto un nombre para mostrar como un nombre exclusivo. Puede editar el nombre para mostrar más adelante.
   - **Grupo federado**: Introduzca el nombre único. Para Active Directory, el nombre único es el nombre asociado con `sAMAccountName` atributo. Para OpenLDAP, el nombre único es el nombre asociado con `uid` atributo.
3. Seleccione **continuar**.

Administrar permisos de grupo

Los permisos de grupo controlan las tareas que los usuarios pueden realizar en el gestor de inquilinos y en la API de gestión de inquilinos.

Pasos

1. Para **Modo de acceso**, seleccione una de las siguientes opciones:
   - **Read-write** (por defecto): Los usuarios pueden iniciar sesión en Tenant Manager y administrar la configuración del inquilino.
   - **Sólo lectura**: Los usuarios sólo pueden ver los ajustes y las funciones. No pueden hacer ningún cambio ni realizar ninguna operación en el administrador de inquilinos o la API de gestión de inquilinos. Los usuarios locales de solo lectura pueden cambiar sus propias contraseñas.

Si un usuario pertenece a varios grupos y cualquier grupo está establecido en sólo lectura, el usuario tendrá acceso de sólo lectura a todos los ajustes y características seleccionados.

2. Seleccione la casilla de verificación **acceso raíz** si los usuarios del grupo necesitan iniciar sesión en el Administrador de inquilinos o en la API de administración de inquilinos.
3. Seleccione **continuar**.

Configure la política de grupo de Swift

Los usuarios de Swift necesitan permiso de administrador para autenticarse en la API REST DE Swift para crear contenedores e ingerir objetos.

1. Seleccione la casilla de verificación **Swift administrator** si los usuarios del grupo necesitan usar la API REST DE Swift para administrar contenedores y objetos.
2. Si está creando un grupo local, seleccione **continuar**. Si está creando un grupo federado, seleccione **Crear grupo** y **Finalizar**.

Añadir usuarios (sólo grupos locales)

Puede guardar el grupo sin agregar usuarios o, opcionalmente, puede agregar cualquier usuario local que ya exista.

Pasos

1. Opcionalmente, seleccione uno o varios usuarios locales para este grupo.

   Si aún no ha creado usuarios locales, puede agregar este grupo al usuario en la página Usuarios. Consulte "Gestionar usuarios locales".

2. Seleccione **Crear grupo** y **Finalizar**.

   El grupo creado aparece en la lista de grupos.

Permisos de gestión de inquilinos

Antes de crear un grupo de arrendatarios, tenga en cuenta qué permisos desea asignar a ese grupo. Los permisos de administración de inquilinos determinan qué tareas pueden realizar los usuarios con el Administrador de inquilinos o la API de gestión de inquilinos. Un usuario puede pertenecer a uno o más grupos. Los permisos son acumulativos si un usuario pertenece a varios grupos.

Para iniciar sesión en el Administrador de arrendatarios o utilizar la API de administración de arrendatarios, los usuarios deben pertenecer a un grupo que tenga al menos un permiso. Todos los usuarios que puedan iniciar sesión pueden realizar las siguientes tareas:

- Vea la consola
- Cambiar su propia contraseña (para usuarios locales)

Para todos los permisos, la configuración del modo de acceso del grupo determina si los usuarios pueden cambiar la configuración y realizar operaciones o si sólo pueden ver la configuración y las características relacionadas.

Si un usuario pertenece a varios grupos y cualquier grupo está establecido en sólo lectura, el usuario tendrá acceso de sólo lectura a todos los ajustes y características seleccionados.

Puede asignar los siguientes permisos a un grupo. Tenga en cuenta que los inquilinos de S3 y los inquilinos de Swift tienen diferentes permisos de grupo.

Permiso	Descripción	Detalles
Acceso raíz	Proporciona acceso completo al administrador de inquilinos y a la API de gestión de inquilinos.	Los usuarios de Swift deben tener permiso de acceso raíz para iniciar sesión en la cuenta de inquilino.
Administrador	Solo para inquilinos Swift. Proporciona acceso completo a los contenedores y objetos de Swift para esta cuenta de inquilino	Los usuarios de Swift deben contar con el permiso de administrador de Swift para realizar cualquier operación con la API REST DE Swift.
Gestione sus propias credenciales de S3	Permite a los usuarios crear y eliminar sus propias claves de acceso S3.	Los usuarios que no tienen este permiso no ven la opción de menú **STORAGE (S3)** > **My S3 access keys**.
Ver todos los cubos	**S3 inquilinos**: Permite a los usuarios ver todas las configuraciones de cubos y cubos. • Inquilinos Swift*: Permite a los usuarios de Swift ver todos los contenedores y configuraciones de contenedores utilizando la API de administración de inquilinos.	Los usuarios que no tienen el permiso Ver todos los cubos o Gestionar todos los cubos no ven la opción de menú **Buckets**. Este permiso se sustituye por el permiso Gestionar todos los cubos. No afecta a las políticas de grupo o bloque S3 utilizadas por los clientes S3 o la consola S3. Solo puede asignar este permiso a grupos de Swift desde la API de gestión de inquilinos. No puede asignar este permiso a grupos Swift mediante el administrador de inquilinos.
Gestionar todos los cucharones	**S3 inquilinos**: Permite a los usuarios utilizar el Administrador de inquilinos y la API de administración de inquilinos para crear y eliminar buckets S3 y para administrar la configuración de todos los S3 buckets en la cuenta de inquilino, independientemente de las políticas de buckets o grupos S3. • Inquilinos Swift*: Permite a los usuarios Swift controlar la consistencia de los contenedores Swift mediante la API de administración de inquilinos.	Los usuarios que no tienen el permiso Ver todos los cubos o Gestionar todos los cubos no ven la opción de menú **Buckets**. Este permiso sustituye al permiso Ver todos los cubos. No afecta a las políticas de grupo o bloque S3 utilizadas por los clientes S3 o la consola S3. Solo puede asignar este permiso a grupos de Swift desde la API de gestión de inquilinos. No puede asignar este permiso a grupos Swift mediante el administrador de inquilinos.

Permiso	Descripción	Detalles
Gestionar puntos finales	Permite a los usuarios utilizar el Gestor de inquilinos o la API de gestión de inquilinos para crear o editar puntos finales de servicio de plataforma, que se utilizan como destino para los servicios de plataforma de StorageGRID.	Los usuarios que no tienen este permiso no ven la opción de menú **Platform services endpoints**.
Utilice la pestaña Consola de S3	Cuando se combina con el permiso Ver todos los cubos o Gestionar todos los cubos, permite a los usuarios ver y gestionar objetos desde la pestaña Consola de S3 en la página de detalles de un bloque.	

Gestionar grupos

Gestione los grupos de arrendatarios según sea necesario para ver, editar o duplicar un grupo y mucho más.

Antes de empezar

- Ha iniciado sesión en el administrador de inquilinos mediante un "navegador web compatible".
- Pertenece a un grupo de usuarios que tiene el "Permiso de acceso raíz".

Ver o editar grupo

Puede ver y editar la información básica y los detalles de cada grupo.

Pasos

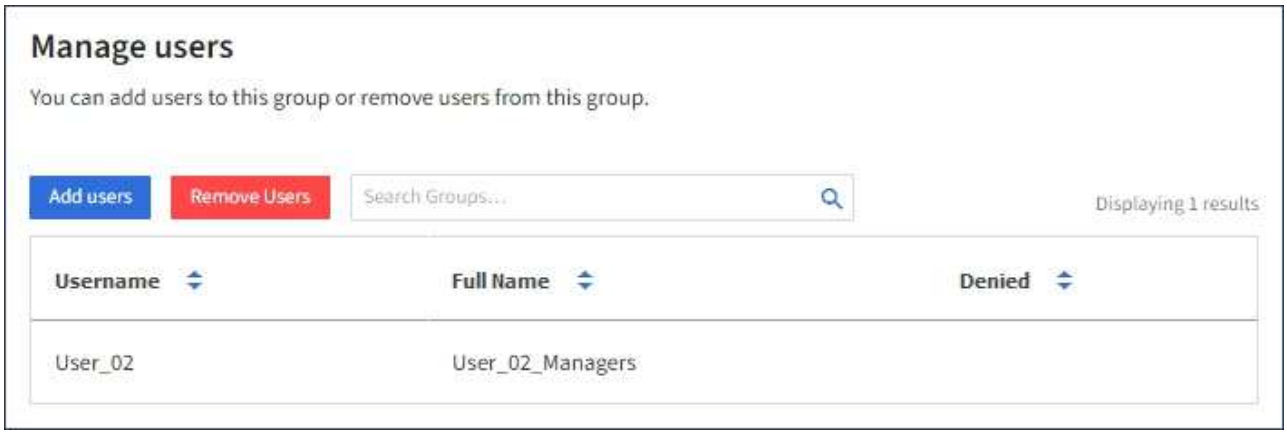
1. Seleccione **ADMINISTRACIÓN de ACCESO** > **grupos**.
2. Revise la información proporcionada en la página Grupos, que muestra información básica de todos los grupos locales y federados de esta cuenta de arrendatario.

   Si la cuenta de inquilino tiene el permiso **Use grid federation connection** y está viendo grupos en la cuadrícula de origen del inquilino:

   - Un mensaje de banner indica que si edita o elimina un grupo, los cambios no se sincronizarán con la otra cuadrícula.
   - Según sea necesario, un mensaje de banner indica si los grupos no se clonaron en el inquilino en la cuadrícula de destino. Puede hacerlo volver a intentar un clon de grupo eso falló.
3. Si desea cambiar el nombre del grupo:
   a. Seleccione la casilla de verificación para el grupo.
   b. Selecciona **Acciones** > **Editar nombre de grupo**.
   c. Introduzca el nuevo nombre.
   d. Selecciona **Guardar cambios.**
4. Si desea ver más detalles o realizar modificaciones adicionales, realice una de las siguientes acciones:
   - Seleccione el nombre del grupo.

- Selecciona la casilla de verificación del grupo y selecciona **Acciones** > **Ver detalles del grupo**.

5. Revise la sección Visión General, que muestra la siguiente información para cada grupo:
   - Nombre para mostrar
   - Nombre exclusivo
   - Tipo
   - Modo de acceso
   - Permisos
   - S3 Política
   - Número de usuarios en este grupo
   - Campos adicionales si la cuenta de inquilino tiene el permiso **Use grid federation connection** y está viendo el grupo en la cuadrícula de origen del inquilino:
     - Estado de clonación, ya sea **Success** o **Failure**
     - Un banner azul que indica que si edita o elimina este grupo, los cambios no se sincronizarán con la otra cuadrícula.
6. Edite la configuración del grupo según sea necesario. Consulte "Cree grupos para un inquilino de S3" y.. "Cree grupos para un inquilino de Swift" para obtener más información acerca de lo que se debe introducir.
   a. En la sección Descripción general, cambie el nombre mostrado seleccionando el nombre o el icono de edición .
   b. En la pestaña **Permisos de grupo**, actualice los permisos y seleccione **Guardar cambios**.
   c. En la pestaña **Política de grupo**, realice los cambios y seleccione **Guardar cambios**.
      - Si está editando un grupo S3, seleccione opcionalmente una política de grupo S3 diferente o introduzca la cadena JSON de una política personalizada, según corresponda.
      - Si está editando un grupo Swift, opcionalmente seleccione o desactive la casilla de verificación **Swift Administrator**.
7. Para añadir uno o varios usuarios locales existentes al grupo:
   a. Seleccione la ficha Usuarios.



   b. Selecciona **Añadir usuarios**.
   c. Seleccione los usuarios existentes que desea agregar y seleccione **Agregar usuarios**.

      Aparece un mensaje de éxito en la parte superior derecha.

8. Para eliminar usuarios locales del grupo:
   a. Seleccione la ficha Usuarios.
   b. Selecciona **Eliminar usuarios**.
   c. Seleccione los usuarios que desea eliminar y seleccione **Eliminar usuarios**.

      Aparece un mensaje de éxito en la parte superior derecha.

9. Confirma que has seleccionado **Guardar cambios** para cada sección que cambiaste.

Grupo duplicado

Puede duplicar un grupo existente para crear nuevos grupos más rápidamente.

> Si su cuenta de inquilino tiene el permiso **Usar conexión de federación de grid** y duplica un grupo de la cuadrícula de origen del inquilino, el grupo duplicado se clonará en la cuadrícula de destino del inquilino.

Pasos

1. Seleccione **ADMINISTRACIÓN de ACCESO** > **grupos**.
2. Seleccione la casilla de control del grupo que desea duplicar.
3. Seleccione **acciones** > **Duplicar grupo**.
4. Consulte "Cree grupos para un inquilino de S3" o. "Cree grupos para un inquilino de Swift" para obtener más información acerca de lo que se debe introducir.
5. Seleccione **Crear grupo**.

Vuelva a intentar clonar el grupo

Para volver a intentar un clon que generó errores:

1. Seleccione cada grupo que indique *(Error de clonación)* debajo del nombre del grupo.
2. Selecciona **Acciones** > **Clonar grupos**.
3. Vea el estado de la operación de clonación desde la página de detalles de cada grupo que está clonando.

Para obtener más información, consulte "Clone los usuarios y los grupos de inquilinos".

Elimine uno o más grupos

Puede eliminar uno o varios grupos. Cualquier usuario que pertenezca únicamente a un grupo que se haya eliminado ya no podrá iniciar sesión en el gestor de inquilinos ni utilizar la cuenta de inquilino.

> Si tu cuenta de inquilino tiene el permiso **Usar conexión de federación de grid** y eliminas un grupo, StorageGRID no eliminará el grupo correspondiente en la otra cuadrícula. Si necesita mantener esta información sincronizada, debe eliminar el mismo grupo de ambas cuadrículas.

Pasos

1. Seleccione **ADMINISTRACIÓN de ACCESO** > **grupos**.
2. Seleccione la casilla de verificación para cada grupo que desee eliminar.
3. Selecciona **Acciones** > **Eliminar grupo** o **Acciones** > **Eliminar grupos**.

Se muestra un cuadro de diálogo de confirmación.

4. Selecciona **Borrar grupo** o **Eliminar grupos**.

Gestionar usuarios locales

Puede crear usuarios locales y asignarles grupos locales para determinar las funciones a las que pueden acceder estos usuarios. El gestor de inquilinos incluye un usuario local predefinido, denominado «root». Aunque puede agregar y eliminar usuarios locales, no puede eliminar el usuario root.

> Si el inicio de sesión único (SSO) está habilitado para el sistema StorageGRID, los usuarios locales no podrán iniciar sesión en el gestor de inquilinos o en la API de gestión de inquilinos, aunque pueden utilizar aplicaciones cliente para acceder a los recursos del inquilino, según los permisos del grupo.

Antes de empezar

- Ha iniciado sesión en el administrador de inquilinos mediante un "navegador web compatible".
- Pertenece a un grupo de usuarios que tiene el "Permiso de acceso raíz".
- Si su cuenta de inquilino tiene el permiso **Use grid federation connection**, ha revisado el flujo de trabajo y las consideraciones para "clonación de usuarios y grupos de inquilinos", y ha iniciado sesión en la cuadrícula de origen del inquilino.

Cree un usuario local

Puede crear un usuario local y asignarlos a uno o varios grupos locales para controlar sus permisos de acceso.

Los usuarios de S3 que no pertenecen a ningún grupo no tienen permisos de administración ni se les aplican S3 políticas de grupo. Es posible que estos usuarios tengan acceso a bloques de S3 otorgado a través de una política de bloques.

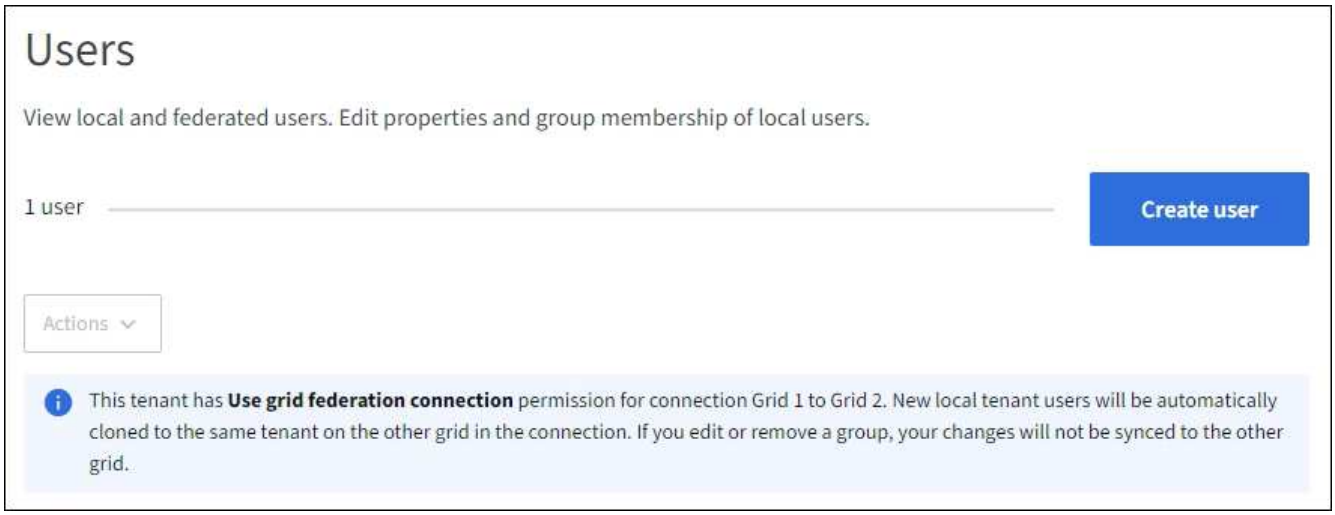
Los usuarios de Swift que no pertenezcan a ningún grupo no tienen permisos de administración ni acceso a contenedor Swift.

Acceda al asistente Crear usuario

Pasos

1. Seleccione **ADMINISTRACIÓN de ACCESO** > **usuarios**.

   Si su cuenta de inquilino tiene el permiso **Usar conexión de federación de grid**, un banner azul indica que esta es la cuadrícula de origen del inquilino. Todos los usuarios locales que cree en esta cuadrícula se clonarán en la otra cuadrícula de la conexión.



2. Seleccione **Crear usuario**.

Introduzca las credenciales

Pasos

1. Para el paso **Introducir credenciales de usuario**, complete los siguientes campos.

Campo	Descripción
Nombre completo	El nombre completo de este usuario, por ejemplo, el nombre y apellidos de una persona o el nombre de una aplicación.
Nombre de usuario	Nombre que utilizará este usuario para iniciar sesión. Los nombres de usuario deben ser únicos y no se pueden cambiar. **Nota**: Si su cuenta de inquilino tiene el permiso **Usar conexión de federación de grid**, se producirá un error de clonación si el mismo **Nombre de usuario** ya existe para el inquilino en la cuadrícula de destino.
Contraseña y confirme la contraseña	La contraseña que el usuario utilizará inicialmente al iniciar sesión.
Denegar el acceso	Seleccione **Sí** para evitar que este usuario inicie sesión en la cuenta de inquilino, aunque todavía pertenezca a uno o más grupos. Por ejemplo, selecciona **Sí** para suspender temporalmente la capacidad de un usuario para iniciar sesión.

2. Seleccione **continuar**.

Asignar a grupos

Pasos

1. Asigne el usuario a uno o más grupos locales para determinar qué tareas se pueden realizar.

   La asignación de un usuario a grupos es opcional. Si lo prefiere, puede seleccionar usuarios al crear o

editar grupos.

Los usuarios que no pertenezcan a ningún grupo no tendrán permisos de administración. Los permisos son acumulativos. Los usuarios tendrán todos los permisos para todos los grupos a los que pertenezcan. Consulte "Permisos de gestión de inquilinos".

2. Seleccione **Crear usuario**.

   Si su cuenta de inquilino tiene el permiso **Usar conexión de federación de grid** y usted está en la cuadrícula de origen del inquilino, el nuevo usuario local se clona en la cuadrícula de destino del inquilino. **Success** aparece como **Cloning status** en la sección Overview de la página de detalles del usuario.

3. Seleccione **Finalizar** para volver a la página Usuarios.

Ver o editar usuario local

Pasos

1. Seleccione **ADMINISTRACIÓN de ACCESO** > **usuarios**.
2. Revise la información proporcionada en la página Usuarios, que muestra información básica para todos los usuarios locales y federados de esta cuenta de arrendatario.

   Si la cuenta de inquilino tiene el permiso **Use grid federation connection** y está viendo al usuario en la cuadrícula de origen del inquilino:

   - Un mensaje de banner indica que si edita o elimina un usuario, los cambios no se sincronizarán con la otra cuadrícula.
   - Según sea necesario, un mensaje de banner indica si los usuarios no se clonaron en el inquilino en la cuadrícula de destino. Puede hacerlo vuelva a intentar un clon de usuario que haya fallado.
3. Si desea cambiar el nombre completo del usuario:
   a. Seleccione la casilla de control para el usuario.
   b. Selecciona **Acciones** > **Editar nombre completo**.
   c. Introduzca el nuevo nombre.
   d. Selecciona **Guardar cambios.**
4. Si desea ver más detalles o realizar modificaciones adicionales, realice una de las siguientes acciones:
   - Seleccione el nombre de usuario.
   - Selecciona la casilla de verificación para el usuario y selecciona **Acciones** > **Ver detalles de usuario**.
5. Revise la sección Visión General, que muestra la siguiente información para cada usuario:
   - Nombre completo
   - Nombre de usuario
   - Tipo de usuario
   - Acceso denegado
   - Modo de acceso
   - Pertenencia a grupos
   - Campos adicionales si la cuenta de inquilino tiene el permiso **Use grid federation connection** y está viendo al usuario en la cuadrícula de origen del inquilino:

- Estado de clonación, ya sea **Success** o **Failure**
- Un banner azul que indica que si edita este usuario, los cambios no se sincronizarán con la otra cuadrícula.

6. Edite la configuración del usuario según sea necesario. Consulte Crear usuario local para obtener más información acerca de lo que se debe introducir.
   a. En la sección Descripción general, cambie el nombre completo seleccionando el nombre o el icono de edición .

      No puede cambiar el nombre de usuario.

   b. En la pestaña **Contraseña**, cambie la contraseña del usuario y seleccione **Guardar cambios**.
   c. En la pestaña **Acceso**, selecciona **No** para permitir que el usuario inicie sesión o selecciona **Sí** para evitar que el usuario inicie sesión. Luego, selecciona **Guardar cambios**.
   d. En la pestaña **Teclas de acceso**, selecciona **Crear clave** y sigue las instrucciones para "Creando las claves de acceso S3 de otro usuario".
   e. En la pestaña **Grupos**, selecciona **Editar grupos** para agregar el usuario a los grupos o eliminar al usuario de los grupos. Luego, selecciona **Guardar cambios**.
7. Confirma que has seleccionado **Guardar cambios** para cada sección que cambiaste.

Usuario local duplicado

Puede duplicar un usuario local para crear un usuario nuevo más rápidamente.

> Si su cuenta de inquilino tiene el permiso **Usar conexión de federación de grid** y duplica un usuario de la cuadrícula de origen del inquilino, el usuario duplicado se clonará en la cuadrícula de destino del inquilino.

Pasos

1. Seleccione **ADMINISTRACIÓN de ACCESO** > **usuarios**.
2. Seleccione la casilla de control para el usuario que desea duplicar.
3. Selecciona **Acciones** > **Usuario duplicado**.
4. Consulte Crear usuario local para obtener más información acerca de lo que se debe introducir.
5. Seleccione **Crear usuario**.

Reintente clonar el usuario

Para volver a intentar un clon que generó errores:

1. Seleccione cada usuario que indique *(Error de clonación)* debajo del nombre de usuario.
2. Selecciona **Acciones** > **Clonar usuarios**.
3. Vea el estado de la operación de clonación desde la página de detalles de cada usuario que está clonando.

Para obtener más información, consulte "Clone los usuarios y los grupos de inquilinos".

Elimine uno o varios usuarios locales

Puede eliminar de forma permanente uno o varios usuarios locales que ya no necesiten acceder a la cuenta de inquilino de StorageGRID.

> Si tu cuenta de inquilino tiene el permiso **Usar conexión de federación de grid** y eliminas a un usuario local, StorageGRID no eliminará al usuario correspondiente en la otra cuadrícula. Si necesita mantener esta información sincronizada, debe eliminar el mismo usuario de ambas cuadrículas.

> Debe utilizar el origen de identidad federado para eliminar usuarios federados.

Pasos

1. Seleccione **ADMINISTRACIÓN de ACCESO** > **usuarios**.
2. Seleccione la casilla de verificación para cada usuario que desee eliminar.
3. Selecciona **Acciones** > **Eliminar usuario** o **Acciones** > **Eliminar usuarios**.

   Se muestra un cuadro de diálogo de confirmación.

4. Seleccione **Eliminar usuario** o **Eliminar usuarios**.